PRIVACY IN PRACTICE:
REIMAGINING HEALTH CARE PRIVACY IN A DIGITIZED WORLD

by
Farnoosh Faezi-Marian

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Bioethics.

Baltimore, Maryland
April 2017

ABSTRACT

As new technologies are introduced to the health care space, such as electronic health records and mobile health applications, there exists a need to address privacy challenges related to new methods of information exchange. Current legal and moral understandings of privacy are insufficient to address the challenges of information privacy. This paper seeks to develop a deliberative framework that allows health policy makers to analyze privacy concerns when introducing or reviewing new technologies or initiatives in order to better protect the values of the American people. In doing so, I review moral and legal perspectives of privacy, arguing that these accounts: (1) fail to incorporate situational context and (2) assume that privacy is always a positive value, and thus, worth protecting at the expense of other goods.

Advisor: Travis Rieder, PhD

Reader: Jeffrey Kahn, PhD, MPH

ACKNOWLEDGEMENTS

It is with profound gratitude that I acknowledge the contributions of my friends, family, and the faculty of the Berman Institute of Bioethics and the Johns Hopkins Bloomberg School of Public Health, without whom this thesis would not have been possible.

In particular, I would like to thank my thesis advisor Dr. Travis Rieder for his enthusiasm, expertise, and willingness to provide feedback at a moment's notice. He added structure and clarity to my thoughts, even when I had trouble articulating them, and he encouraged me to engage with difficult literature and concepts, even when it would have been easier to point me in a different direction.

I would also like to thank my reader Dr. Jeffrey Kahn for his time, diligence, and responsiveness. His insightful feedback elevated this work and challenged me to think more deeply about the issues at hand.

I am indebted to my friends and classmates Diana Mendoza Cervantes and Cameron Okeke. We were inseparable over the past two years, encouraging each other to be better students, friends, and people. I am pleased to say that I have found lifelong friends in both, and I wish them every success in the future.

Finally, I am grateful to my parents for their steadfast love, support, and encouragement as I worked to fulfill the requirements of this degree. Throughout my life they have inspired me to be a better version of myself, to work harder to achieve my goals, and to never settle for less. I hope I have made them proud.

TABLE OF CONTENTS

Intended to be blank.

INTRODUCTION

As new technologies are introduced to the health care space, there exists a need to address privacy challenges related to new methods of information exchange, such as the exchange of electronic health records and the use of mobile health applications. Current legal and moral understandings of privacy are insufficient to address the challenges of information privacy. This paper seeks to develop a deliberative framework that allows health policy makers to analyze privacy concerns when introducing or reviewing new technologies or initiatives in order to better protect the values of the American people. In doing so, I review moral and legal accounts of privacy, and through the exploration of two case studies, argue that these accounts: (1) fail to incorporate situational context and (2) assume that privacy is always a positive value, and thus, worth protecting at the expense of other goods.

By appropriately identifying concerns related to new technologies or initiatives, policy makers are poised to predict acceptable trade-offs to privacy. Trade-offs are driven by (1) circumstance, (2) comfort and ease, and (3) expectation, because society has adopted new methods of conducting old activities. Privacy is a value that is sometimes trumped by other values in the form of trade-offs. If policy makers can better predict the tensions that require consideration in the context of these trade-offs, they are better positioned to

develop more effective policies that accomplish goals without unduly burdening members of society.

PRIVACY PERSPECTIVES

For any given definition of privacy, there exist circumstances for which definitions are inadequate. For example, in its better-known iteration, privacy has been defined as the "right to be let alone" (Warren & Brandeis, 1890); however, critics have argued that this definition is limited in scope. For instance, information about someone can be spread without his or her awareness, so perhaps privacy also includes the ability to control information about oneself. Moreover, there are situations that require active engagement of the person, such as in the sharing of electronic health records with appropriate parties; simply leaving someone alone will not solve all privacy challenges in an ever-changing socioeconomic landscape.

Privacy has been described as possessing a chameleon-like quality, adapting to circumstances as they arise (BeVier, 1995). "Perhaps the most striking thing about the right to privacy," Judith Jarvis Thompson suggests, "is that nobody seems to have any very clear idea what it is" (Thomson, 1975). There exist numerous definitions of privacy out of a necessity to capture the many circumstances that present challenges to privacy. A single definition of privacy may be common to a discipline or field, but that definition may become

inadequate outside the scope of its original context. For instance, privacy defined as noninterference does not help us grapple with the challenges of sharing personal health information with people other than our physicians; rather, we can turn to privacy defined as the control of personal information to address potential concerns that arise from sharing health information. As new situations arise, our understanding of privacy must evolve as well. We cannot simply rely on existing accounts of privacy to address new challenges. Even the token metaphor for discussing the importance of information privacy falls short. In George Orwell's *1984*, Big Brother is a metaphor for totalitarian government surveillance; however, this literary portrayal of a world with no privacy does not adequately capture concerns related to the storage of personal data in large databases. Below, I will discuss a few moral and legal conceptions of privacy and their limitations. Before doing so, I will discuss the value of information privacy in particular.

The Value of Information Privacy

Although the concept of privacy is not straightforward, privacy itself is valuable and worth protecting. In most cases, protecting privacy put limits on power, increases individual autonomy, builds trust in relationships, and protects rights. Jeroen van den Hoven offers the most comprehensive normative view of information privacy by sorting moral reasons to protect privacy into four categories: (1) information-based harm, (2) informational inequality, (3)

informational justice, and (4) encroachment on moral autonomy (Van den Hoven, 2001). He arrives at these categories "by asking what gives moral legitimacy to public policy that would restrict the collection, retrieval, and dissemination of data […] because it furthers moral ends, prevents harms, and promotes equality, justice, and autonomy" (Van den Hoven, 2001). In the interest of simplicity, I will briefly discuss the first two categories because they are the most relevant to the case studies explored in this paper.

Information-based harms can result from access to information available through public government records. For example, before the Driver's Privacy Protection Act (DPPA) of 1994, which restricted the disclosure of personal information, anti-abortion activists would harass abortion providers and patients through the use of public driving license databases (Hammitt, 1997). In this instance, policy makers restricted the retrieval of personal information from driver's records for the purposes of preventing harm.

Informational inequality results when shared information disproportionately benefits some people, but not others (Van den Hoven, 2001). In the age of data aggregation and data mining, individuals are not equipped with the same tools and access to their public information as companies are, thus creating an imbalance of power. Companies have more leverage over individuals, simply because they have the resources to accrue and analyze information. A possible solution to this disparity is to democratize databases, which ultimately allows for more transparency, though this solution must be

weighed against potential negative outcomes of democratized databases, such as in the DPPA case. A more narrow approach would be to allow individuals to access only their own records. Individuals can view and correct information about themselves, and thus have more control over their information.

Unlike the DPPA case, information gleaned from these databases is novel in the way it is aggregated; people are not accruing data about themselves in the way that companies do. Because companies are able to aggregate data in a sophisticated way, they know more about an individual's online habits than the individuals themselves. The disparity in knowledge between companies and the individual means that companies can use information about an individual's habits to subconsciously manipulate them into buying goods or clicking on certain articles. For example, consider the noticeable rise in fake news throughout and after the 2016 United States presidential election.[1] Although it is impossible to confirm whether fake news stories generated by websites or hackers influenced the results on the election, Facebook has taken measures to combat fake news by fact-checking headlines through third-party sources such as Politifact, The Associated Press, and Snopes (Ortutay, 2016). Rather than simply filtering out fake news, Facebook has flagged disputed news for its users so that they are aware of which news is unverified and likely fake. Because users are now equipped with more information than was previously available to them,

[1] Fake news is news that is unverified or false.

they can decide for themselves whether or not they want to click on a news article.[2]

Some scholars argue for the existence of a right to privacy, whereas others deny it (Schoeman, 1984). Others claim that privacy is merely derivative of other rights. Judith Jarvis Thomson most famously argues for the latter point, stating: "I don't have a right to not be looked at because I have a right to privacy; I don't have a right that no one should torture me in order to get personal information about me because I have a right to privacy; one is inclined, rather, to say that it is because I have these rights that I have a right to privacy" (Thomson, 1975). For Thomson, privacy is derivative in its importance; I agree with her claim. Rights to privacy can be expressed more clearly through invoking liberty rights, property rights, or any other more fundamental rights. The wrongness of violations of privacy can be explained through the existence of other rights, without ever invoking privacy. For example, if a man is tortured for personal information, his right not to be tortured has been violated. If a woman's pornographic picture is stolen from her safe, her right to her property has been violated. Thomson explains that other rights already protect the consequences that a right to privacy tries to protect. To invoke privacy adds nothing to the argument to protect a man from torture. He should be protected because he has a right to not be tortured, not because he has a right to privacy. Regarding

[2] Fake news is targeted and is usually the result of past browsing history. Fake news amplifies potentially false beliefs held by individuals by consistently reinforcing these beliefs through the spread of false information (Ortutay, 2016).

information, Thomson argues that we have not violated someone's right to privacy by knowing something about him or her. Rather, she states: "We have a right that certain steps shall not be taken to find out facts, and we have a right that certain uses shall not be made of facts" (Thomson, 1975). Improper dissemination of an electronic health record should be prevented, not because the patient has a right to privacy, but because patients have a right that their health data shall not be used for purposes outside of what was intended when it was collected; providers must ask for consent in order to disseminate patient health information, even if the medical institution owns the data found in the electronic health record.

Accounts of Privacy and Their Limitations

Privacy is most commonly discussed in the context of harms (Calo, 2011). A harm has occurred when an individual is worse off than they were before an action took place. For example, if your physician shares your health information with insurers and, as a result of that exchange, your insurance premiums rise, you have been harmed. You are worse off because your insurance has gotten more expensive. Not all cases of privacy violations result in harms, however. A wrong is a violation of a right. Perhaps the most popular understanding of a privacy violation is the case of the Peeping Tom. In the original tale, Tom "stole a look at Lady Godiva as she rode naked through the streets as a condition that her

husband, the king, would cease to impose backbreaking taxes on the town" (Calo, 2011). Tom was subsequently blinded for peeking.

A Peeping Tom, or voyeur, refers to someone who seeks sexual gratification through spying on people. For example, they may peek into windows or through webcams to watch unsuspecting people undress or engage in sexual acts. Even if the Peeping Tom's activity goes unnoticed, the observations acquired during his peeping are not disseminated, and the person has not been made worse off than they were before the action took place, the person who is being spied on is wronged because a right has been violated. According to Thomson, knowing something about someone is not a violation of their right to privacy; however, seeking that information by means of spying on them is a violation of that person's right that certain methods should not be undertaken to find out facts about them.

The Peeping Tom case does not help us work through all information privacy cases since there may not be a dissemination of private information beyond the Peeping Tom. As discussed earlier, the cornerstone of information privacy discussions is the dissemination of information. In his seminal work, legal scholar Daniel Solove discusses two metaphors for privacy, in particular, focusing on information privacy. Big Brother is always watching in George Orwell's *Nineteen Eighty-Four*. Orwell's story describes a totalitarian state that is ruled by Big Brother, a "monolithic power engaged in massive surveillance" (Calo, 2011). It is the token metaphor for discussing information privacy.

While useful for discussing the consequences of surveillance, the Big Brother metaphor falls short when exploring other aspects of information, such as storing electronic health information in databases. As a solution, Solove proposes that Kafka's *The Trial* be used as a metaphor to discuss database concerns. Briefly, *The Trial* tells the story of Joseph K., who is inexplicably arrested one morning. He does not know why he has been arrested, and more troubling, the officers that inform him of his arrest do not know either. In its purest sense, the epistemic plight of Joseph K. is a harm. It is important to note that a harm or wrong need not be tied to a human actor, but instead can be committed through automated decision making (Calo, 2011). According to Solove, "*The Trial* captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life. At any time, something could happen to Joseph K.; decisions are made based on his data, and Joseph K. has no say, no knowledge, and no ability to fight back" (Solove D. , 2001). Structural harms and wrongs can be committed, and even if not individually felt, can collectively weaken social cohesion, trust, transparency, and other values society may find important.

The potential for structural harms and wrongs increases with rapid technological advancements in health. One such example, which I will discuss later, is the Precision Medicine Initiative, which seeks to aggregate the health

data of one million participants in order to create a representative registry of Americans that can be studied by researchers.

Legal History of Privacy

At least since the 18th Century, Western conceptions of privacy have changed, and much of this change has been driven through United States case law.[3] Privacy is not explicitly protected in the Constitution of the United States, which was signed in 1787 and amended most recently in 1992. In all the years that the Constitution has been the highest law of the land, a beacon of American values, and the protector of liberties, not once has it been amended to explicitly protect privacy. James Madison penned the first ten amendments to the Constitution, named the Bill of Rights, in order to expand constitutional protections for State and individual liberties. These amendments limited the Federal Government's power to intrude upon certain liberties, granting such legal protections as freedom of religion, freedom to assemble peacefully, the right to bear arms, freedom from unreasonable search and seizure, freedom from double jeopardy, and a right to a fair trial. The aforementioned list is not exhaustive, a fact that is captured by the Ninth Amendment to the Constitution: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people" (U.S. Const. amend. IX). That is

[3] For the purposes of this paper, I have narrowed the scope of this discussion to Western conceptions of privacy. Even within Western literature, discussions of privacy are nuanced and diverse; I would not be able to satisfactorily engage with non-Western conceptions of privacy, though they exist. Despite this limitation, my deliberative framework takes into account the context in which privacy is situated and, thus, can also be used in non-Western policy making.

to say, while privacy protections may not be explicitly written in the Constitution, people may still have a right to privacy. The Supreme Court has upheld rulings to protect privacy, however, citing the penumbra, or shadowy spaces, of the Constitution in Griswold v. Connecticut, 381 U.S. 479 (1965), and later the Due Process Clause, drawn from the Fifth and Fourteenth Amendments to the Constitution.

Griswold v. Connecticut overturned a state law that criminalized the use of contraceptives within a marriage, ruling that such a law violated the right to marital privacy. Justice William Douglas wrote the majority opinion, writing that "specific guarantees in the Bill of Rights have penumbras, formed by the emanations from those guarantees that give them life and substance," Griswold v. Connecticut, 381 U.S. 479, 480 (1965). From these guarantees, Justice Douglas argues, there are zones of privacy, such as marital privacy, that should not be intruded upon by the courts. Justice Black and Justice Stewart wrote the dissenting opinion, arguing that the right to privacy does not exist because it is not written in the Constitution, Griswold v. Connecticut, 381 U.S. 479, 508 (1965) (Black and Steward, J.J., dissenting). Justice Black states: "I like my privacy as well as the next one, but I am nevertheless compelled to admit that government has a right to invade it unless prohibited by some specific constitutional provision" 381 U.S. 479, 501 (1965) (Black and Steward, J.J., dissenting).

Justice Goldberg wrote the concurring opinion, drawing from a different justification but agreeing with the Court's opinion, stating: "To hold that a right

so basic and fundamental and so deep-rooted in our society as the right of privacy in marriage may be infringed because that right is not guaranteed in so many words by the first eight amendments to the Constitution is to ignore the Ninth Amendment and to give it no effect whatsoever," Griswold v. Connecticut, 381 U.S. 479, 492 (1965) (Goldberg, J., concurring). As previously explained, the Ninth Amendment states that "[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people" (U.S. Const. amend. IX). In summary, Justice Goldberg's argument is that just because the right to marital privacy is not spelled out in the Constitution, does not mean that such a right is not held by the people. While Justice Goldberg's argument is not a popular defense of privacy to this day, he does point to a moral right to privacy, one that is deeply entrenched in society, if not in law. Here, there is a clear distinction between legal rights and moral rights. Justice Goldberg is pointing to what he believes is a moral right, a right to marital privacy, that he believes should be protected, even when it is not explicitly mentioned in the Constitution.

Griswold v. Connecticut was a hallmark case that set the precedent for privacy being invoked in cases of sex and reproduction. For example, the right to possess birth control for married couples was extended to unmarried couples in Eisenstadt v. Baird, 405 U.S. 438 (1972) due to the Equal Protection Clause of the Constitution. The Court stated: "If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted

governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child," Eisenstadt v. Baird, 405 U.S. 438, 454 (1972). Subsequently, Roe v. Wade, 410 U.S. 113 (1973) extended the right to privacy under the Due Process Clause of the Fourteenth Amendment to include a woman's decision to have an abortion. Finally, in Lawrence v. Texas, 539 U.S. 558 (2003), a law prohibiting same-sex sexual contact was overturned, with the Court again citing the Due Process Clause of the Fourteenth Amendment. Justice O'Connor wrote the concurring opinion, stating that the Texas law touches "upon the most private human conduct, sexual behavior, and in the most private of places, the home," Lawrence v. Texas, 539 U.S. 558, 568 (2003) (O'Connor, J., concurring). Griswold v. Connecticut was even cited in the recent ruling Obergefell v. Hodges, 576 U.S. ___ (2015), making same sex marriage legal across the United States.

So far, none of the aforementioned court cases have been overturned. Constitutional purists will continue to argue that the right to privacy does not exist because it is not written in the Constitution, only erroneously inferred. Upon reviewing these cases, it seems that the constitutionally recognized right to privacy is protection from governmental intrusion into private spaces. That is, these rulings have pointed to public and private spaces, a dichotomy that is prominent in legal discourse (Nissenbaum, 2009). According to Nissenbaum, "[t]here seems to be general agreement […] that although the terms private and public vary in meaning from one arena to another […], they invariably

demarcate a strict dichotomy" (Nissenbaum, 2009). Private space is intimate and personal, typically referring to the home, while public space is beyond the home where people can come together to discuss civics, such as in Habermas's *Öffentlichkeit*, or "public sphere" (Habermas, 1989). What is done in public can be controlled to a degree based on the interests and values society, but what is done in private, or in the home, should only concern those parties involved. It is this public/private dichotomy that has historically driven conversations related to privacy. What is done in public can be openly critiqued and constrained, as public space is shared by all members of society and should reflect the values of that society as a whole. What is done in private, however, is up to the individual, since they do not share this space with anyone but themselves and whomever they invite inside. This familiar dichotomy has evolved due to the emergence and dominance of the Internet. There now exists a prominent public space that is accessed from the private and stores private information. This new dimension bridges the gap between the private and the public, facilitating the flow of information between spheres. Since information privacy concerns largely center around the flow of information, it is particularly important to consider this dimension when developing policies that seek to protect information that is shared.

I will conclude this section on the legal history of privacy, which is in no way exhaustive, with what is perhaps the most popular conception of privacy in law. In the influential article titled "The Right to Privacy," published in 1890,

Samuel Warren and Louis Brandeis state: “It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is” (Warren & Brandeis, 1890). In exploring past case law to define privacy, Warren and Brandeis point to a “right to be let alone” (Warren & Brandeis, 1890). Warren and Brandeis conclude, "the principle which protects personal writings and any other productions of the intellect or the emotions, is the right to privacy" (Warren & Brandeis, 1890). While the “right to be let alone” may be the foundation of privacy law, and may fit within the construct of the public-private dichotomy defined by the courts, it fails to address the new challenges brought about by emerging technologies. For example, the “right to be let alone” may take into account concerns over surveillance technologies, but it does not consider government transparency in posting Federally funded research, or access to public health registries to promote research, examples I will discuss later.

REIMAGINING INFORMATIONAL PRIVACY IN HEALTH POLICY

Privacy cannot be discussed in isolation, for it is the context in which privacy is situated that determines the values at stake, and thus, the morally appropriate course of action to take when considering trade-offs to privacy. Privacy as an abstract concept is unhelpful when the stakes are high, as they are

in health care and in health policy. In the health care space, violations of privacy can lead to devastating consequences, such as denial of health insurance coverage, debilitating fees, and loss of agency. Invoking privacy is not sufficient to protect what ought to be protected, nor is it sufficient to identify what ought *not* be protected. By invoking privacy without context, policy makers risk painting the situation at hand with too broad a brush, failing to protect or promote actual values at stake, while limiting the effectiveness of an initiative due to too many unnecessary restrictions.

Privacy will continue to evolve as new technologies are introduced, and as new initiatives take hold, resulting in even more conceptions of privacy than currently exist. The problem with many conceptions of privacy becomes apparent when we invoke privacy, but fail to understand someone else's understanding of privacy. For example, privacy can be defined as the control of information or the "right to be let alone." If accessing health data is the goal of an initiative, privacy defined as the control of information lends itself to different opportunities for trade-offs than if privacy is defined as the "right to be let alone." For instance, the initiative may choose to de-identify all health data submitted in order to protect individuals from being contacted by researchers who would like to study their data or ask for additional health data. The initiative would be appealing to the individual's right to be let alone, even at the risk of hindering scientific breakthroughs. On the other hand, if privacy requirements are fulfilled by individuals controlling their own information, some

identifiable information may be tied to their health data so that researchers could reach out for follow-ups; at the very least, there would be a mechanism in place to reach these individuals should researchers express interest in engaging with their data. The justifications provided for trading off an individual's privacy for access to their health data must be more compelling in the former case because the individual has a stronger claim to their privacy (as the right to be left alone). If privacy is defined as the control of personal information, then contacting the individual before engaging with their health data is acceptable, if not required. Policies will be shaped by how strong a claim individuals have to privacy. Hence, clarifying the context, or circumstances, becomes a vital first step prior to recommending policies that protect privacy in a given situation.

Privacy has and will continue to change, so we must be able to identify these changes and analyze what values are at stake in light of these changes. As previously discussed, Western conceptions of privacy have been shaped by case law; societal norms have also played a role in shaping these conceptions. Helen Nissenbaum's framework of contextual integrity seeks to provide a metric from which changes in societal norms can be measured. She states that contextual integrity "is preserved when informational norms are respected and violated when informational norms are breached" (Nissenbaum, 2009). Nissenbaum goes on to explain that these informational norms are characterized by: (1) contexts, which include roles, power structures, norms, and values, (2) actors, (3) attributes, and (4) transmission principles, or to whom or where information is

now shared as a result of a change in practice. In creating this framework, Nissenbaum helps us two-fold. First, contextual integrity helps us identify deviations from the norm, and thus, helps us predict if and when new technologies, policies, or initiatives are disruptive. Second, contextual integrity can help us understand why this disruption will or has occurred by breaking down the many factors that play into a change in the status quo. By anticipating and understanding anxieties felt by stakeholders (those who have vested interest in an activity), policy makers can work to temper concerns as a result of disruptive changes by recommending policies that address stakeholder concerns, while simultaneously promoting the values espoused in an activity's mission statement and societally-held values.

In its current state, the policy making process follows the principles of contextual integrity to a degree. That is, policy makers are tasked with understanding the current narrative surrounding existing technologies and the potential impact of new or repurposed technologies. For example, before regulations are approved by the Office of Management and Budget, they undergo an economic impact analysis in order to estimate their impact on the American economy; the analysis prescribed by Circular A-4 is regimented and standard to all regulations (Office of Management and Budget, 2003). Policy makers are tasked with creating implementation scenarios that take into account anticipated stakeholder reactions, existing standards and norms in the industry, missing gaps that can be addressed by a new regulation, and ultimately, are

tasked with proposing an option that will be the least disruptive while still being the most effective in accomplishing the goals of the Administration. Although the components of the contextual integrity framework exist, policy making is more art than science. There is no formula that policy makers can apply to a situation that will result in the best outcome; a good deal of judgment is at play. Contextual integrity can help policy makers think about policies in a more regimented way, thereby increasing the likelihood that all possible sticking points are considered.

Contextual integrity has its limitations, however, as Nissenbaum is first to admit. It is very similar to the concept of reasonable expectation that is used in the courts. For example, when I am out in public I know that other people see me. I do not mind being seen by others because I have the reasonable belief that I will be forgotten. That is, even if others see me, they are most likely to forget me immediately and move on. The introduction of cameras on every street corner was disruptive to this reasonable expectation of being forgotten. Now, as I walk down the street, I am aware that while other people will forget me, there are cameras that will record me. The reason that society has accepted this disruption of the norms is because cameras add at least the perception of safety, if not demonstrable increases in safety. It is understood that these cameras help police officers do their jobs better. If someone has gone missing, street cameras are used to identify when they were last seen in public. If there has been a hit and run, street cameras can help identify the perpetrator. The trade-off of having our

reasonable expectation of being forgotten infringed upon is a society that is better able to respond in cases of wrong doing in public spaces. Reasonable expectation, like contextual integrity, is based on current societal norms. So while helpful in identifying deviations from these norms, it is not helpful is making value judgments about these deviations. Just because something deviates from the norm, or violates contextual integrity, does not mean it is less aligned with our values as a society. In fact, a deviation from the norm may be necessary to get us closer to realizing our values.

Merely recognizing that new events or initiatives disrupt privacy norms is not sufficient. Privacy is multifaceted, as evinced by the many conceptions of it that exist. Common to these conceptions of privacy, however, is the notion that privacy is inherently good and must be protected or promoted. Often, at least in informational privacy, it is the value against which other values are assessed, and the value that is necessarily infringed upon when trade-offs are made. For example, there is still a contentious debate surrounding the disclosure of a patient's HIV status to their partners. Although there have been trade-offs made in promoting public health to the detriment of personal privacy, such as the requirement for doctors to report certain infections to public health registries, the HIV disclosure debate illustrates how current these conversations still are. At least in this case, it is debatable whether public health trumps the right to privacy over personal medical information.

Privacy is not always good, however. In the context of informational privacy, control of information can be good or bad, as I will explain later through an example involving open source data. This observation brings me to the vital second step of understanding privacy. Again, the first step is to understand the context, which can be done diligently through the contextual integrity framework. The second step of understanding privacy is deciding if privacy is promoting a good within a given context. If privacy is value neutral, then it is not worth promoting at the expense of competing values. If privacy is working against values that are held by society, steps must be taken to mitigate privacy's negative influence.

Some critics argue that privacy itself does not change, but society's tolerance for privacy violations changes. As people become more comfortable with a new normal of privacy, they amend their understanding of a perceived loss of privacy to reflect this new normal. In the context of health, medical records have become digitized; this reflects a change in the state of affairs that people have not explicitly consented to. Rather, institutions deemed a transition to electronic records necessary, and users of the health care system have been required to adapt to the new normal. Yes, it seems that tolerance has changed. This change is especially evident in younger generations in their apparent disregard of privacy as they contribute to social media websites and use mobile applications to stream music, order delivery, and hail a cab. In contrast, older generations may resist these technologies because they never normalized their

use; those adventurous enough to join Facebook, for example, may first seek advice or assistance from children and grandchildren. Even institutional interpretations of privacy have changed, even though the Supreme Court uses the same source material to review cases.

Tolerance has changed our relationship to privacy, but I reject that it is the sole driver of this change. Through tolerance of new technologies or approaches, we may be willing to accept changes counter to our beliefs, values, or habits in favor of a desirable outcome; or we may simply be resigned to a new state of affairs.[4] To tolerate something is to accept it begrudgingly, to embrace something is to accept it enthusiastically. Embracing a new technology or approach means that we willingly seek out these changes, integrate them into our lives, and implore others to consider doing the same. In the context of online banking, I can tolerate the move from paper statements to electronic statements by not complaining to my bank when the change occurs, or by not asking that my bank continue paper statements in lieu of electronic. Or, I can embrace online banking and, in addition to receiving electronic statements, set up payment alerts through my mobile application and cash checks without ever stepping foot into a bank.

[4] Due to regulatory requirements, clinicians and hospitals must use electronic health record technology in lieu of paper records. People must tolerate this change to receive health care in the United States since there is no going back to paper records. Similarly, our use of credit cards is changing. Due to recent regulations, merchants must adopt credit card chip readers lest they be held accountable for fraudulent charges (rather than credit card companies). United States merchants currently accept signatures and chips with signatures; many other countries require a chip and a Personal Identification Number (PIN) (Newman, 2016).

People are becoming more comfortable using social media, online dating and shopping, and using applications that gather information, including health information (e.g., FitBit). In fact, people are seeking out these services because they make life better in some way. Rather than wait in line at a fast food restaurant, I can order ahead on a mobile application and pick up my order at the counter; the trade-off for my privacy is more time to do something else. Sometimes I prefer traditional sit-down restaurant food, but do not want to leave the house. Restaurants typically do not deliver, but there is an "app" for that. I can order sit-down restaurant food through a third-party application and tip someone to wait for my food and deliver it to me; the trade-off for disclosing my address to a stranger is convenience.

Institutions play a large role in ensuring our relationships with technology remain positive, despite the reality of less privacy. For instance, I am more likely to use my credit card to make purchases online if my credit card company protects me from fraud, or reimburses me when fraud has occurred. Having institutional protections in place allows me to enjoy the benefits of technology without having to be overwhelmingly concerned about the loss of my privacy.

As a society, we are embracing new norms for new trade-offs. As each new technology is introduced, there are corresponding pros and cons to adopting the technology. Younger generations are generally early adopters of new technologies, embracing the benefits of social media (staying in touch with friends), online shopping (not having to leave the house to buy goods), and

mobile applications despite the trade-offs to their privacy. Older generations may be reluctant to participate in these technologies because they prioritize privacy. While older generations may be concerned by younger generations' cavalier attitude toward individual privacy, younger generations may view older generations' reluctance to accept trade-offs to individual privacy as unnecessarily uptight – a relic of an outdated way of thinking and a failure to embrace new norms. Because younger generations worry about privacy less, they have access to certain goods and services that remain untapped by those who are reluctant to make the trade.

CASE STUDIES

The Precision Medicine Initiative

Establishing a statistically significant and representative database for research purposes has the potential to further public health. The Precision Medicine Initiative's (PMI) long-term objective is to help researchers better understand and assess disease risk, mechanisms, and therapies (Collins & Varmus, 2015). Advances in bioinformatics and information technology have enabled researchers to analyze and store incredible amounts of data. Data scientists aspire to extract information from millions of individuals in order to generate algorithms that will help predict clinical needs for each patient. Not only does this approach have clinical significance for individuals, it also will allow health care institutions to better predict and plan for the health needs of

the communities they serve (Hood & Friend, 2011). Moreover, scientists may be able to predict the health burden of a community and plan educational, environmental, or policy interventions (Hood & Friend, 2011). Large sample sizes are integral to assessing public health-level need. In order to achieve the aforementioned, active participation by the PMI cohort is essential; thus, the PMI endeavors to "pioneer new models for doing science that emphasize engaged participants and open, responsible data sharing" (National Institutes of Health, 2015). To that end, the Director of the National Institutes of Health, Francis Collins, tasked the PMI Working Group with developing a blueprint for the design and execution of the PMI Cohort Program (PMI-CP). The PMI Working Group released "The Precision Medicine Initiative Cohort Program – Building a Research Foundation for 21st Century Medicine" on September 15, 2015, a 100 page document that explored the many facets of PMI, including data privacy. The Working Group made the following recommendations to protect data privacy:

> **Recommendation 5.31**: The PMI-CP should create and use de-identified data for research whenever feasible to do so.
>
> **Recommendation 5.32**: The PMI-CP should engage data privacy experts to create an effective combination of technology and policy to minimize risks of re-identification of de-identified data.

Recommendation 5.33: The PMI-CP should develop educational materials for participants that explain the principles of data privacy, its limitations, and their role in helping to maintain it.

Recommendation 5.34: The PMI-CP should have a clearly articulated plan in case of a privacy breach, which includes notification to participants. (Precision Medicine Initiative Working Group, 2015)

From these recommendations, it appears that privacy is at odds with data sharing, especially when it comes to potentially re-identifiable health information. These recommendations point to three specific privacy goals: (1) de-identification, (2) restricted access, and (3) notifying affected parties in the event of a data hack or breach. The Working Group specifically asks policy makers to create policies that minimize the risks of data re-identification. At face value, this is a vague request. The PMI Working Group acknowledges that de-identified data is re-identifiable as a result of the mission of PMI. Collecting as many data points as PMI strives to collect for the purposes of research has consequences; these data can be cross-referenced to publicly available data, thereby increasing the likelihood that individuals can be identified. Moreover, PMI will collect genetic information, which may be identifiable based on rare markers. Also, consider that researchers will have to reach out to individuals for consent if they seek to assemble smaller cohorts, such as those with a rare disease phenotype; researchers engaging in broader studies can use de-identified data, as there will

likely be a provision that gives broad consent to researchers to study de-identified data.

From the concerns articulated by the PMI Working Group, it seems inevitable that data will be re-identified, but it is what happens after the fact that will matter most to participants. The PMI-CP is voluntary. It is likely that those participating in the program do not mind sharing their information in the name of science. Instead, participants are likely more concerned with what happens to their health data outside of the research setting, as they have only consented to their data being used in the research setting. Despite the seeming inevitability of re-identification, intentional or otherwise, the PMI Working Group continues to recommend de-identifying data as a means of protecting information from nefarious parties. As a way of reducing the risk of de-identification, the PMI Working Group has recommended that the PMI-CP "discourage data from being copied outside the PMI secure computing environment, while allowing outside data to be imported into the PMI cohort computing environment" (Precision Medicine Initiative Working Group, 2015). By maintaining data in a secure computing environment, the PMI Working Group believes there is less chance of re-identification, and thus, a reduced likelihood that identifiable data will be distributed. While this approach seems reasonable at first glance, it is shortsighted and does not adequately address the concern of re-identified data falling into the wrong hands. Rather than developing a policy to discourage data exports, a more effective policy that gets to the root of participant anxiety is this:

Access to data will be restricted to authorized personnel only and will only be used for authorized purposes; the sale of data to third parties is prohibited. Clarifying their values, the White House released the "Precision Medicine Initiative: Privacy and Trust Principles," which included the following guidance: "Data access, use, and sharing should be permitted for authorized purposes only. Certain activities should be expressly prohibited, including sale or use of the data for targeted advertising" (The White House, 2015). Based on the two guidance documents discussed here, it is clear that privacy, in the context of PMI, points to a particular value: the right to not be used to make a profit. What violates privacy in this case, is not re-identifiable data, but third parties using data collected by PMI to make a profit at our expense. Protecting privacy within the context of PMI promotes a good, the right to not be used to make a profit, and furthers the interests of PMI, which is to promote research that benefits public health without causing undue burden to participants.

Open Data and the Environmental Protection Agency

This next example offers a look at privacy working as a negative influence in the pursuit of values that promote transparency, community engagement, and creativity. That is, by appealing to privacy, specifically understood as the control of information, we are not promoting values that society finds important and worth protecting. Open data is information freely available to anyone who can access it. The idea behind open data in government is to provide constituents

with data collected by agencies so that they may in turn analyze the data and come up with novel solutions to address challenges faced in the United States and abroad. In short, two (or many) heads are better than one. Another goal of open data is transparency; the Obama Administration created https://open.whitehouse.gov for this purpose, though they also encouraged and hosted "hackathons," events that bring together computer programmers to solve challenges using open data sets (The White House, 2013).

Recently, the Trump Administration has come under fire for its lack of transparency, a value that was held by the former administration (The White House, 2013). The evidence for this enduring value is clear, even constrained within government: constituents calling for public officials to release tax returns to highlight conflicts of interests, requiring that public employee salaries be accessible to the public, preserving all Presidential and Vice Presidential records, and allowing the public to request access to government records, codified by the Freedom of Information Act.

Prior to President Trump's inauguration, the following headlines were plastered across the Internet: "Scientists are frantically copying U.S. climate data, fearing it might vanish under Trump" (Washington Post), "Rogue Scientists Race to Save Climate Data from Trump" (Wired), and "Why is federal government data disappearing?" (The Hill). Initially, these outcries were seen as overreactions, but nevertheless, computer programmers held events to save as much publicly available data as possible, and reportedly, federally employed

scientists scrambled to back up climate data in the last days of the Obama Administration (Eilperin, Rein, & Fisher, 2017). These actions were not remiss, it seems, as the Trump Administration has been noticeably antagonistic towards the Environmental Protection Agency (EPA), even nominating Scott Pruitt as Administrator (it is worth noting here that Administrator Pruitt has sued the EPA many times, and at one point, championed its elimination as an agency). Shockingly, the Trump Administration issued a gag order for government agencies, such as the National Parks Service, and a media blackout for the EPA (Rott, 2017). The scientific community immediately noticed that open data sets had been removed from the open data website established by former President Obama, leaving only a blank template for promoting transparency. The open data sets are still preserved on the archived White House site, a requirement of the Presidential Records Act that does not allow Presidential records to be deleted, but they are stored in difficult to read formats.

During Presidential transitions, the new Administration is given leeway to reorganize information and content on White House websites to reflect Administration priorities. Many associated pages and links have been deleted because they do not reflect Administration priorities, which is the prerogative of any new Administration. The Federal Government, to a degree, gets to decide what it shares with the public. In this sense, the Federal Government is protecting its privacy by controlling the flow of information that it manages. The right to privacy is not limited to individuals; it also includes groups, companies,

and governments. For example, companies are allowed to have trade secrets. The Coca-Cola Company's recipe is a trade secret, which means that the company will never have to disclose the famous Coca-Cola recipe to the market; patent protections, on the other hand, would require that the recipe be disclosed in 20 years. It comes to no surprise that governments have secrets as well. Security clearance is required for national security positions, and disclosure of these secrets is called treason. There are whistleblower protections in place, however, so that Federal employees can report agency misconduct without fear of retaliation.

So it seems that government actions that promote privacy for the government work against values that the American people value, namely, transparency and access to federally funded research (i.e., taxpayer funded research). The control of information can be good in cases of protecting medical information from insurers so that insurance premiums do not rise, but bad in terms of the government promoting transparency in federally funded research and establishing trust with its constituents. Context matters, and the value we place on privacy matters.

ACCEPTABLE TRADE-OFFS TO PRESERVE THE MOST IMPORTANT VALUES

We must be careful of assigning blanket legal protections to privacy.

Simply basing decisions on the need to protect privacy does not get to the root cause of concerns felt by society, such as appropriate access to information, knowing how information will be used, and knowing when information is being collected. By painting too broad a brush with policies that point to protecting privacy, we may wrongly protect what ought not to be protected, as in the case of health data for the purposes of research. In doing so, we risk stagnating progress, as discussed in the Precision Medicine case study. PMI seeks to transform how medicine is practiced in the United States, shifting health care from reactive to preventative. This transformation, if successful, will have an enormous impact on the quality of life for Americans, will overhaul the American health care economy, and will contribute to the scientific literature. By simply aiming to protect privacy, we lack the precision to identify real causes for concern in the PMI. For example, de-identifying all data to protect participant privacy is likely going a step too far if the real concern for PMI participants is that their data may end up in the wrong hands (e.g., insurance companies). Instead, a more nuanced approach may yield policies that require researchers to seek permission from an institutional review board before acquiring identifiable data for use in research studies.

Without a more nuanced approach to tackling disruptive technologies and endeavors, we may also fail to acknowledge what must be protected. For example, seemingly innocuous open databases may result in harassment and stalking of individuals, such as in the case of public driving license databases.

Had policy makers taken into account the political and social landscape of the time, they may have predicted that anti-abortion activists and women who had received abortions would be targeted by groups seeking to do them harm. In another example presented by the open data and EPA case, respecting an institution's privacy may have debilitating effects on innovation. Privacy should not be seen as value neutral or positive in all circumstances. It is important to evaluate the value of privacy within context, determining privacy's positive or negative influence based on its impact on other values that are worth protecting. In this case, respecting institutional privacy contributes to a lack of transparency, especially in the context of federally funded research – research that should ideally be accessible to everyone since the public funds it.

Despite knee-jerk concerns, we are willing to trade individual entitlements to privacy for other pursuits that are important to us, such as public health and access to federally funded research on climate change. Public opinion regarding acceptable invasions of privacy waxes and wanes; 9/11 prompted a desire to increase surveillance in the name of fighting terrorism. The USA PATRIOT Act was signed into law 45 days after 9/11, beginning a string of policies that increased government surveillance. We became resigned to taking off our shoes at airports and submitting to invasive full body scans, all in the pursuit of national security, and in turn, our personal safety. A decade later, the National Security Agency documents leaked by Edward Snowden exposed a different public opinion. People were outraged by the scope of surveillance by the

government, suggesting that there are limitations to encroaching upon privacy for the sake of combating terrorism. This shift in public opinion was once again reflected in Apple's legal battle with the Federal Bureau of Investigation, refusing to create a "backdoor" that unlocks all iPhones (for criminal and terrorist cases); Apple stated: "We believe security shouldn't come at the expense of individual privacy" (Apple, 2016). Apple may have overstated the case for privacy protections, especially since we trade privacy for security in many contexts; thus, we may more reasonably state that security should not come at too great an expense of individual privacy.

In the context of information sharing, health information is both shared and withheld. Individual privacy between patient and physician in the clinical context does not exist once the patient willingly discloses medical information– information is shared between clinicians, technicians, and labs in order to promote the patient's health. Perhaps this expanded notion of the health care team can include informaticists and researchers for, in the context of precision medicine, they are promoting the health of the patient. Doctors are required to submit infectious disease data to registries in order to protect public health at the expense of their patient's anonymity. Physicians have access to Prescription Drug Monitoring Programs (PDMPs) that allow them to look up "doctor shoppers," or patients who visit multiple doctors in the hopes of getting prescribed opioid painkillers; at least in Oregon, access has been expanded to include pharmacists and police officers with a warrant (McCarty, et al., 2015).

Contact tracing is another example of elevating public interests over individual privacy, even if the case in question does not have widespread public health consequences. Mental health information must be reported to authorities in cases where there is risk of harm to another person. On the other hand, while allowing patient access to health records is required of health care providers, mental health information can be kept from patients to prevent psychological harm.

Trade-offs are driven by (1) circumstance, such as in the wake of 9/11 and in light of new technologies, (2) comfort and ease, such as through online shopping, and (3) expectation, because society has adopted new methods, as in the adoption of electronic medical records. Privacy is a value that is sometimes trumped by other values in the form of trade-offs. If policy makers can better predict the tensions that require consideration in the context of these trade-offs, they are better positioned to develop more effective policies that accomplish goals without unduly burdening members of society. At the very least, these policies will be permissible; at best they will be laudable.

BIBLIOGRAPHY

Apple. (2016, February 16). *Government Information Requests*. Retrieved February 25, 2016, from Privacy: http://www.apple.com/privacy/government-information-requests/

Bennett, C. J. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States.

BeVier, L. R. (1995). Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection. *William & Mary Bill of Rights Journal , 4* (2), 455-506.

Calo, R. (2011). Boundaries of Privacy Harm. *Indiana Law Journal , 86*, 1131-1162.

Collins, F., & Varmus, H. (2015). A New Initiative on Precision Medicine. *New England Journal of Medicine , 372* (9), 793-795.

Eilperin, J., Rein, L., & Fisher, M. (2017, January 31). *Resistance from within: Federal workers push back against Trump*. Retrieved from The Washington Post: https://www.washingtonpost.com/politics/resistance-from-within-federal-workers-push-back-against-trump/2017/01/31/c65b110e-e7cb-11e6-b82f-687d6e6a3e7c_story.html?utm_term=.b6607af1c5b5

Habermas, J. (1989). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society.* (T. Burger, & F. Lawrence, Trans.) Cambridge, Massachusetts: MIT Press.

Hammitt, H. (1997, November 30). *States to Feds: We Don't Want Your Legislated Privacy*. Retrieved February 15, 2017, from http://www.govtech.com/templates/gov_print_article?id=100553389

Hood, L., & Friend, S. (2011). Predictive, personalized, preventive, participatory (P4) cancer medicine. *Nature Reviews. Clinical Oncology. , 8* (3), 184-187.

Kasper, D. V. (2005). The Evolution (or Devolution) of Privacy. *Sociological Forum, 20* (1), 69-92.

McCarty, D., Bovett, R., Burns, T., Cushing, J., Glynn, M. E., Kruse, S. J., et al. (2015). Oregon's strategy to confront prescription opioid misuse: A case study. *Journal of Substance Abuse Treatment , 48* (1), 91-95.

McCloskey, H. (1980). Privacy and the Right to Privacy. *Philosophy , 55* (211), 17-38.

National Institutes of Health. (2015, April). *What are some of the challenges facing precision medicine and the Precision Medicine Initiative?* Retrieved February 2016, from Genetics Home Reference: https://ghr.nlm.nih.gov/primer/precisionmedicine/challenges

Nehf, J. (2003). Recognizing the Societal Value in Information Privacy. *Washington Law Review* , 1-91.

Newman, L. H. (2016, July 20). *Why You Still Can't Use a Chip Card Everywhere*. Retrieved from Slate: http://www.slate.com/articles/technology/future_tense/2016/07/why_you_still_can_t_use_a_chip_card_everywhere.html

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford: Stanford University Press.

Office of Management and Budget. (2003). *Circular A-4.*

Ortutay, B. (2016, December 15). *Facebook gets serious about fighting fake news*. Retrieved from The Associated Press:

http://bigstory.ap.org/article/22e0809d20264498bece040e85b96935/facebook-takes-fake-news

Precision Medicine Initiative Working Group. (2015). *The Precision Medicine Initiative Cohort Program – Building a Research Foundation for 21st Century Medicine.*

Rott, N. (2017, January 25). *Media Blackout Ordered For EPA Employees During Trump Transition*. Retrieved March 2, 2017, from National Public Radio: http://www.npr.org/2017/01/25/511554855/media-blackout-ordered-for-epa-employees-during-trump-transition

Schoeman, F. (1984). Privacy: Philosophical Dimensions. *American Philosophical Quarterly , 21* (3), 199-213.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review , 154* (3), 477-560.

Solove, D. (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review , 53* (6), 1392-1462.

The White House. (2013). *Open Government Initiative*. Retrieved from https://obamawhitehouse.archives.gov/open

The White House. (2015). *Precision Medicine Initiative: Privacy and Trust Principles.*

Thomson, J. J. (1975). The Right to Privacy. *Philosophy and Public Affairs , 4* (4), 295-314.

Van den Hoven, J. (2001). Privacy and the Varieties of Information Wrongdoing. In R. A. Spinello, & H. Tavani (Eds.), *Readings in CyberEthics* (pp. 488-500). Sudbury, MA: Jones and Barlett Publishers.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review , IV* (5), 193-220.

CURRICULUM VITAE

Farnoosh Faezi-Marian is a Master of Bioethics candidate at the Johns Hopkins Bloomberg School of Public Health and the Berman Institute of Bioethics. She received her B.S. in Biology at the University of Virginia in 2013. As a student at UVA, she worked at Madison House as the Head Program Director of Medical Services. After graduation, Farnoosh worked at the Virginia Information Technologies Agency as a staff administrator and researcher for the Health Information Technology Standards Advisory Committee (HITSAC). She currently works in the Health Division of the White House Office of Management and Budget. Her research interests include issues of privacy, security, and consent relating to large data systems, especially in their use as analytical tools for research and policy development.